AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A Black Samsung cell phone seized from Brijesh Shah in the custody of United States Pretrial Services at 85 Marconi Blvd., Room 512, Columbus, Ohio.

Case No. 2:21-mj-528

APPLICATION FOR A SEARCH WARRANT BY TELEPHONE OR OTHER RELIABLE MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

A Black Samsung cell phone seized from Brijesh Shah in the custody of United States Pretrial Services at 85 Marconi Blvd., Room 512, Columbus, Ohio, as described in Attachment A hereto,

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2251(a)(e), 2252A(a)(2) and (b)(1); 2422 (b); and 2261A(2)	Production of Child Pornography, Receiving Child Pornography, Online Enticement and Cyberstalking

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

CHAD LAPP, Special Agent, FBI
Printed name and title

Sworn to by telephone or other reliable means at 3:20 a.m./p.m. in accordance with Fed. R. Crim. P. 4.1.

Date: August 6, 2021

Judge's signature

City and state: Columbus, Ohio

Elizabeth Preston Deavers, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched is a Black Samsung cell phone that was seized from Brijesh Shah and is currently located in the custody of United States Pretrial Services at 85 Marconi Blvd Room 512, Columbus, Ohio.

ATTACHMENT B

Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 2251(a)(e) (Production of Child Pornography) and 18 U.S.C. § 2252A(a)(2) and (b)(1) (Receiving Child Pornography), 18 U.S.C. § 2422(b) (Online Enticement), and 18 U.S.C. § 2261A(2) (Cyberstalking) and involve Brijesh Shah since February 2014, including:

a. Evidence of internet usage for the production, transportation or possession of child pornography as defined in 18 U.S.C. § 2256, including dates and times of usage; IP addresses; and user names and passwords used to access the internet or any accounts via the internet;

b. All visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, including all motion pictures or digital video clips containing such visual depictions;

c. All video recordings which are self-produced and pertain to sexually explicit images of minors, or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

d. All records and information, including written or electronic correspondence or communications, pertaining to the production, transportation, shipment, distribution, receipt, trade, sale, purchase, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or any attempt to commit any such offense;

e. All records or information that pertain to offers to transmit, the solicitation of a transmission, or the transmission, through interstate or foreign commerce by any means (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

f. All records or information naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet;

h. All records or information referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, transporting, receiving, or possessing child pornography as defined in 18 U.S.C. § 2256, including chat logs, call logs, address books or contact list entries, and digital images sent or received;

i. All images and video clips of child erotica, defined as material or items that may be sexually arousing to persons having a sexual interest in children but that are not in and of themselves legally obscene and do not depict minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256, such as images of minors depicted in underwear or partially undressed; and

j. Storage media used as a means to commit or facilitate the violations described above.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history. Records evidencing the use of the Internet, including:

a. Records of Internet Protocol addresses used.

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging storage media and computer-assisted scans and searches of the storage media, that might expose many parts of the storage media to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the

warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time-period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the storage media do not contain any data falling within the ambit of the warrant, the government will return the storage media to its owner within a reasonable period of time following the search and will seal any image of the storage media, absent further authorization from the Court.

8. The government may retain the storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the storage media and/or the data contained therein if evidence falling within the ambit of the warrant is found.

9. The government will retain a forensic image of the storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss: AFFIDAVIT OF CHAD LAPP

Affidavit in Support of an Application Under Rule 41 for a Warrant to Search and Seize Evidence Including Digital Evidence

I, Chad Lapp, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since December 2014. My current assignment is to the Portland Division, Bend Resident Agency. I received 21 weeks of training at the FBI Academy in Quantico, Virginia. My responsibilities include the investigation of federal criminal offenses, to include Production of Child Pornography, Receiving Child Pornography, Online Enticement, and Cyberstalking.

2. I submit this affidavit in support of an application for a search warrant for a Black Samsung Cell Phone that was seized by United States Pretrial Services in the Southern District of Ohio from Brijesh S. Shah (hereinafter "Device") currently maintained in the Custody of United States Pretrial Services in the Southern District of Ohio at 85 Marconi Blvd Room 512, Columbus, Ohio 43215, which is further described in Attachment A. As set forth below, I have probable cause to believe that the Device contains evidence, fruits, and instrumentalities, as set forth in Attachments B hereto, of violations of 18 U.S.C. § 2251(a)(e) (Production of Child Pornography) and 18 U.S.C. § 2252A(a)(2) and (b)(1) (Receiving Child Pornography), 18 U.S.C. § 2422(b) (Online Enticement), and 18 U.S.C. § 2261A(2) (Cyberstalking).

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from

other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. As noted above this investigation concerns the alleged violations of the following:

a. 18 U.S.C. § 2251(a)(e) (Production of Child Pornography) provides in part, that whoever employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so shall be fined and imprisoned not less than 15 years nor more than 30 years.

b. 18 U.S.C. § 2252A(a)(2) and (b)(1) (Receiving Child Pornography) provides in part, that whoever, knowingly receives any child pornography that has been mailed, or using any

means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempts or conspires to do so shall be fined and imprisoned not less than 5 years and not more than 20 years.

c. 18 U.S.C. § 2422(b) (Online Enticement) provides in part, that whoever, using the mail or any facility or means of interstate or foreign commerce knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined and imprisoned not less than 10 years or for life.

d. Title 18 U.S.C. § 2261A(2)(Cyberstalking) provides in part, that whoever, with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or, any other facility of interstate or foreign commerce to engage in a course of conduct that causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to that person, an immediate family member of that person, or a spouse or intimate partner of that person shall be fined an imprisoned for not more than 5 years.

Statement of Probable Cause

5. On 12/07/2016, the FBI Bend Resident Agency began working with the Harney County Sheriff's Office (HCSO) on an investigation of Brijesh S. Shah of Columbus, Ohio, who was suspected of violating state laws, Oregon Revised Statute (ORS 163.432) Online Sexual Corruption of a Child in the Second Degree and (ORS 163.433) Online Sexual Corruption of a Child in the First Degree with a minor, who will be referred to as KD in this affidavit. In 2017

the District Attorney's Office in Harney County referred the case over to the Department of Justice and the FBI to investigate. I reviewed the FBI case file which includes HCSO reports, FBI reports that summarize victim and witness interviews, FBI reports that summarize the review of digital evidence, data obtained via administrative subpoenas, and an affidavit for a search warrant signed on 03/24/2017 by Special Agent Clayton Smith and United States Magistrate Judge Paul Papak. On 08/02/2021, I received a United States Government Memorandum regarding a violation of release conditions that involved the Device targeted by this affidavit. Relevant facts supporting an application for a search warrant are described below.

Harney County Sheriff's Investigation

6. On 10/14/2016, Harney County Sheriff's Office (HCSO) Deputy Chris Nisbet was informed by police dispatch that Anna Defenbaugh had dropped off several items at the HCSO. These items were in the possession of her minor daughter, KD. The items included a Wonder Woman greeting card, a Samsung cell phone, and a U.S. Postal Priority envelope addressed to KD at Crane High School, which contained a letter that provided instructions to KD on how to contact Shah.

7. Defenbaugh reported to HCSO that KD attended Crane High School, 43277 Crane Venator Lane, Crane, Oregon. Since the Defenbaughs lived on a working ranch 2.5 hours from the school, KD lived at the Crane High School dormitory during the week and traveled home on the weekends. A few weeks before she collected the items, Defenbaugh learned from KD that she had been in contact with Shah and that the contact began in 2014, when KD was 14 years old.

8. The U.S. Postal Priority envelope with an enclosed letter collected by Defenbaugh

was addressed to KD, 43277 Crane Venator Lane, Crane, Oregon, which is the Crane High School address. The sender's mailing address was listed as 14363 Northwest Tradewind Street, Portland, OR and the postage stamp on the envelope was post marked on 9/30/2017 from Columbus, Ohio. The enclosed typed letter asked KD, why she hadn't used the Samsung phone, he had sent to contact him. The letter instructed KD to contact him by using any web browser on a desktop, laptop, tablet or phone to text him using the username UltraKassi and password Sugardaddy on a website textfree.us. He also provided KD with his email address of missmybabygirl@outlook.com and his telephone number (614)304-1975 and requested that she text or call him at the number. The letter ended, "I am going insane here, miss you like crazy!!! Love Daddy."

9. Defenbuagh (KD's mother) described conversations she had with KD, where KD disclosed that she and Shah had been in contact by text and telephone calls beginning in approximately February 2014. Defenbaugh reported that KD said she spoke to Shah using her cell phone on just a few occasions to number (823)276-9624, but routinely communicated with Shah by texting. Defenbaugh said KD stated that Shah also made threats to KD and that if KD did not do what he wanted KD to do, he was going to hurt KD's little brother and KD's family. Defenbaugh said KD said she thought Shah was possibly of eastern decent because he sounded like he was from India. Defenbaugh said she seized all of KD's electronic devices approximately in March 2014 to end KD's communication with Shah. However, when Defenbaugh saw the items in her daughter's dorm room in October 2016, she realized the contact had started again.

10. Defenbaugh said KD received a hand-written letter from Shah, which listed his full name, Brijesh Shardul Shah with cell phone (832)276-9624. In the letter Shah provided KD

with his username Brijeshsshah and password Monster800 for websites: Hi5, Tagged.com, and KIK.com, as well as his email address at Brijeshsshah@hotmail.com. Defenbaugh said KD told her KD never communicated with Shah on Hi5 or Tagged.com or his email at Hotmail.com. Defenbaugh stated KD said she mainly used KIK.com and texted using Shah's cell phone (832)276-9624. Defenbaugh said she collected a second package sent to KD which was a box containing a blanket. Defenbaugh said the box was sent by U.S. Postal Priority mail and addressed to KD's address at Crane High School, 43277 Crane Venator Lane, Crane, Oregon. The sender's mailing address was 14363 Northwest Tradewind Street, Portland, Oregon and the postage stamp on the envelope was post marked 11/23/2016 from Columbus, Ohio.

11. Defenbaugh said based on a review of KD's cell phone, she saw Shah's profile name for KIK.com was Monster800 and a profile picture of a yellow sports motorcycle. Defenbaugh also saw text messages between KD and Shah as well as some pictures on KD's phone. One picture was of KD showing her cleavage and bra. Defenbaugh read some text messages sent by Shah where he referred to KD "darling" and "sweetie." Defenbaugh said Shah instructed KD to delete the photos and text and to send him confirmation the photos and text were deleted. Defenbaugh said by reviewing KD's cell phone, it indicated KD called the telephone number (823)276-9624. Later in the investigation, Shah told HCSO deputies that his personal cell, a Samsung Galaxy Edge used the phone number (823) 276-9624.

HCSO responds to Crane High School about a suspicious adult on campus

12. On 12/6/2016, HCSO Deputy Matt Ellibee and Deputy Dan Jenkins responded to a call of a suspicious adult male hanging out at the Crane High School. Deputy Ellibee interviewed Crane High School official Gwen Haigh. Haigh said there was a "middle eastern"

adult male hanging around the Crane High School dormitory and seen driving a black SUV bearing Oregon license plate 441 JHP. Furthermore, Haigh stated there had been a "middle eastern" male at the Crane High School on two different occasions on December 5th and 6th, 2016. On one of the days, the adult male attended a basketball game and on the other day, he was seen hanging around the parking lot near the dormitory. Haigh told investigators she confronted the "middle eastern" adult male on 12/6/2016, at approximately 1800 hours near the Crane High School dormitory. During the contact, Haigh asked the adult male for his identification and he provided his Ohio Driver's license. The adult male told Haigh he had lost his credit card while at the Crane High School basketball game and was looking for the school office to report the loss. Haigh told the adult male he needed to leave the premises and he did. Haigh became aware that KD had been in an online relationship with a "middle eastern" adult male from talking with Defenbaugh shortly after the Crane High School basketball game. On 12/5/2016, Defenbaugh and KD attended the basketball game at Crane High School because Defenbaugh's son played in one of the games.

13. Haigh recalled that she received a telephone call on 12/6/2016 at approximately 0600 hours while at the dormitory. Haigh believed the person she spoke with on the telephone was of "middle eastern" descent due to his accent and he had a high-pitched voice. The caller claimed to be from the Amazon company and wanted to speak with KD regarding the delivery of a package. Haigh did not allow the person to contact KD.

Forensic Interview of victim KD

14. KD was forensically interviewed on 12/20/2016. During this interview KD described her interactions with Shah. KD said that in approximately August 2014, she was given

a cell phone by her parents. Not long after receiving the phone, she said she began receiving text messages and a few calls from a boy, who claimed to be 14 years old. They boy had a high-pitched voice and he said his name was Brijesh Shah and he wanted to be friends. KD said Shah told her that he learned about KD form CJ (a friend of KD's from school), and KD believed that CJ had put KD's name and telephone number on a dating website without KD's knowledge. KD said the dating website lister her age as 18 years old. KD said that when KD and Shah first began texting, KD told Shah she was 14 years old. KD said she recalled he said he was either 14 or 15 years old and that he lived in Columbus, Ohio. KD continued to describe their texting and how KD described her family, where she went to school, and that they lived in Fields, Oregon. KD said she told Shah that she was very close to her little brother. Later, KD said Shah asked to have a picture of KD's face and she sent it. KD said that a few weeks later, Shah sent her a picture of his face and she realized that he wasn't a 14-year-old boy, but an older adult male. KD described Shah as balding, hairy, with brown skin and approximately 40 years old. KD said that when KD initially found out how old Shah was KD asked him why he lied about his age and Shah said he didn't want KD to dislike him for being older.

15. KD said that after Shah sent his picture to KD, he became more aggressive and asked for three pictures of her face each day. She said Shah then began to demand naked pictures of her. She said she complied and sent nude pictures of her bare breasts by attaching the pictures to text messages. She said KD told Shah, she didn't want to send nude photos because it was wrong. KD said Shah got mad at KD and stated he would hurt KD's little brother and family if she didn't send them. She described how Shah went further and told KD wouldn't see her little brother again unless she sent more nude pictures to him. She said Shah instructed KD to take

nude pictures of her "pussy" and requested photos of her in certain poses, and she complied. She stated that Shah told her to take pictures of her masturbating, and she complied by putting her fingers into her vagina and took pictures and sent them to Shah. She said Shah sent nude pictures of himself standing in front of a mirror to KD. KD stated she saw his naked hairy body, including his penis, pot belly and skinny legs. She said that anytime she stopped sending pictures to him, Shah threatened her by saying he knew where KD and her family lived, and he would hurt KD's family. KD said the pictures were exchanged by attaching them to text messages.

16. KD said that after talking to Shah for approximately three months, KD's mother took all her electronic devices away because Defenbaugh saw Shah's name in her cell phone contact list. KD said she and Shah stopped communication for several months after her mother took her devices. KD said after her mother took her devices, Shah sent a package to KD, which included a cell phone. KD said whenever they stopped communicating, Shah sent unsolicited items to her at Crane High School. KD said one package included vitamins, pain pills, and a blue blanket. Shah told KD that he wanted her to be healthy with perfect hair, perfect skin, and a perfect body, so he sent the pills. KD said she threw all these items away.

17. During her freshman year at Crane High School, KD got an iPod from a friend, and she opened a KIK account and she used her real name on her profile and her username was Doobie4me. KD used her real name on her profile so her other friends could communicate with her on KIK.com. KD said that since KD used her real name, Shah was able to find her and they began communicating again. KD said Shah texted KD with messages, "where are you," "I miss you," and "I love you." KD said Shah told her not to tell anyone about him because if he got caught, he would hurt KD and her family and he knew where they lived. KD said it was scary

because Shah said that he was watching her.

18. KD said Shah told her that once she turned 18, she could move to Columbus, OH to attend college and live with him. She said Shah often told KD that he traveled to Portland to visit his friends. She said he asked if they could meet, and KD said no. She stated Shah instructed KD to text him fantasy stories about sexual encounters with two guys and one girl or two girls and one guy. KD said she attempted to text Shah sexual fantasies but she had no experiences with sex, so she said they were "dumb" stories. She said Shah told KD that when she attended college in Columbus, OH they would have sexual encounters with two guys and two girls, as well as perform bondage. She said Shah remined KD to be very careful and to not tell anyone about their text and picture swapping. KD said her last contact with Shah was in September 2016 using the website KIK.com.

Interview of Brijesh Shah

19. Based on HCSO's investigation, Deputy Jenkins and Deputy Ellibee conducted an interview with Shah at the Crystal Crane Hot Springs Motel, 59315 Highway 78, Burns, OR, on 12/6/2016. Outside the motel was a black SUV bearing an OR license plate 441 JHP. Shah told officers he had a date of birth of 2/2/1974 with a home address of 2262 Summit Street, Columbus, Ohio and his cell phone number was (832) 276-9624.

20. Shah explained he recently flew from his hometown of Columbus, Ohio to visit his friend Kush Pathak in Portland, Oregon. Shah said during his visit, Pathak was too busy working to visit with him and Pathak told Shah to visit the Malheur National Forest in Southeastern Oregon. Shah followed his GPS and got lost in the area because his boss called him, which caused Shah to take a wrong turn and ended up at the Crane High School by mistake

instead of the Malheur National Forest. While at the school, he asked for directions to Malheur National Forest. However, because it was so late, he didn't travel to the National Forest and decided to stay at Crystal Crane Hot Springs Motel for the night and planned to return to Portland at a later date. On the next day, Shah spoke to a clerk at the Crane store about the sights to see in town. Shah was told to go to a basketball game being played at the Crane High School gym. Shah attended the game and then returned to the Crane store. Shah realized he had lost one of his credit cards at the basketball game and returned to Crane High School and walked over to the school dorm to ask about his lost credit card. As he walked into the dorm, Shah was approached by a woman at the school wanting to know why he was there. Shah explained the loss of the credit card to her. Shah provided his Ohio driver's license to the woman for his identification.

20. Shah told the deputies, he did not know anyone in the area and was not trying to meet or communicate with anyone in the area. Shah was told by the deputies, a person in Crane had been receiving packages with a return mailing address of Portland, OR and U.S. post mark from Ohio. Shah said he knew nothing about the packages. Shah was told a 15-year-old girl had been contacted by a person with a similar name as Shah's and received packages from Portland with postage from Columbus, Ohio. Shah said it wasn't him. Shah said he was not communicating with anyone in Crane. Shah admitted he was involved in using dating websites that operated similar to Facebook named HI5.com also known as TAGGED.com. Shah said he been on the site since 2000 and had met with lots of women from the site including women in Bend and Portland, Oregon. Shah explained the conversations he had on the site with women were usually "explicit." Shah used his laptop and showed the Deputy his profile, which was a

picture of a yellow sports motorcycle and his profile name was Brijesh S. Shah. Shah was asked about having any contact with any girls from the Crane, Oregon area and he said if she was on TAGGED, he might have been in contact with her or exchanged nude photographs. Shah offered to have the Officers go through his computer and his cell phone. Shah asked Deputy Dan Jenkins if he needed legal representation. Deputy Jenkins told Shah it was up to him whether he wanted representation and if it made him more comfortable, he would read him his Miranda rights. Deputy Jenkins then read Shah his Miranda rights. Shah said he understood his rights and agreed to continue to talk to the Officers. Again, Shah offered Deputy Jenkins his laptop and cell phone for inspection.

21. Shah was asked if he knew KD. Shah responded that he knew several "Kassis" from the TAGGED website. Shah was told KD received photographs from Shah that were nude form the neck down via the internet and KD sent Shah photographs nude from the neck down. Shah said you have to be 18 years old to be on the website. Shah said he sent his photograph to numerous people. Deputy Jenkins said that KD texted/exchanged photos with a person with a name similar to Brijesh Shah. Deputy Jenkins then advised Shah, he was under arrest for online sexual corruption of a child and he read him his Miranda rights a second time and seized Shah's laptop and cell phone.

22. On 12/7/2016, HCSO Deputy Chris Nisbet contacted Shah's attorney Martin Thompson and advised that HCSO was applying for a search warrant to search Shah's vehicle. Thompson spoke to Shah and he agreed to provide consent to search the vehicle. Deputy Nisbet conducted a consent search of Shah's vehicle with Shah and attorney Thompson present. Shah informed Deputy Nisbet that everything in the vehicle was his and that he had not been traveling

with anyone. Deputy Nisbet located a backpack in the vehicle and collected a Best Buy receipt dated 12/4/2016 for the purchase of an iPod touch and iPod touch case, an American Airline purchase receipt for a change fee for Brijesh Shah, a brand new iPod Touch, 10 Trustex condoms, handwritten instructions to drive to Hotsprings, an Econolodge hotel receipt, an iPod touch case, three American Airlines boarding passes for Brijesh Shah, a Starbucks receipt, and handwritten instructions to drive to Crane High School – "3rd left follow past school behind school park by door gym."

Interview of Kushagra Pathak

23. The FBI interviewed Shah's friend Kushagra Pathak in Portland, Oregon. Pathak and Shah had been friends for several years and met in college. When Pathak first moved to Portland, OR his home address was 14363 NW Tradewind Street, Portland, OR. As previously mentioned in the affidavit, the packages sent to KD at the Crane High School had Pathak's home address of 14363 NW Tradewind Street, Portland OR. Pathak stated he and Shah vacationed together in Hawaii from 11/25/2016 to 12/3/2016. Shah had flown from Columbus, Ohio to Hawaii to meet Pathak and his family. While Shah was in Hawaii, he told Pathak he had been talking to someone, who was 21 or 22 years old and planned to go meet her when they all flew back to Oregon. Pathak told Shah to make sure to check her identification just to be safe. Pathak said when they returned from Hawaii on 12/3/2016, Shah rented a vehicle and drove to Crane, Oregon. Pathak said he never told Shah he was too busy to visit with Shah and did not tell Shah to go visit the Malheur National Forest. Pathak had no knowledge of the two packages mailed to KD in Crane, OR and he did not know KD.

Review of Digital Devices

24. Pursuant to a search warrant signed by United States Magistrate Judge Paul Papak data extracted from Shah's Samsung Galaxy Note Edge cell phone was reviewed. The Facebook messenger data in the phone showed three messages from the phone to KD. From 9/1/2016 through 9/6/2016, Shah asked KD "Did u get it," "hope u come on IG or kik soon," and "where r u???" The KIK messenger data in the phone showed several communications between Shah and KD. On 9/17/2016, Shah told KD "I would rather have seen u in bed" and "Its been awhile." KD then asked, "What do you want." Shah replied "I want to love you forever." KD responded "You have me forever." Shah responded "I mean with me in person." On 9/17/2016, Shah stated "U have such a cute butt." KD responded that Shah is a "perv." Shah then tells KD "That's why you love daddy. Is that what you are going to sleep in." KD responded, "I'm freezing at night I couldn't wear that." Shah states, "You are my sweetie. GN and DS baby girl. Daddy loves you." The WhatsApp data in the phone showed messages between Shah and Pathak. On 12/6/2016, Shah reported to Pathak that he arrived at Crystal Crane Hot Springs, 58315 Hwy 78, Burns, Oregon with telephone number (541) 493-2312. Shah told Pathak, "she" is 15 minutes from Shah's location. Shah took a video of the Crane Hot Springs and the hotel. Pathak asked Shah, "Where is your friend in the video fucker?" She coming back or was your limp dick too disappointing." Shah responded, "She had to leave for work." "Fuck u and yes she is coming back." The SMS Message data in the phone showed communications between Shah and Pathak. On 11/11/2016, Shah messaged Pathak, "Will be renting a car while I am there. Might be going to see that girl in Crane, Oregon for a couple of days if her schedule permits." In the contacts of the phone KD's name was listed with two telephone numbers and the address 43277 Crane-

Venator Lane, Crane, Oregon. Shah also attached a picture of KD's face in the contact list. The web history data of the phone showed that beginning on 12/1/2016 through 12/6/2016, Shah searched for "Crane elementary school," "Crane union high school," and "crane high school dorms, crane, Oregon." The image data of the phone showed numerous images of KD's face and sexually explicit images of female genitals.

25. Data extracted from an iPod touch used by KD were reviewed. Within the images there were numerous pictures of KD's face, a naked bottom and female torso wearing a bra and jean shorts. There were also images of KD's bare breasts. There were also numerous images of KD in various poses. The poses included KD wearing a bathing suit top and bottom and the pictures were focused on her breasts. Other poses included KD completely naked lying on a bed, KD touching her genital area with her hand and a curling iron, and images of KD naked in a shower. Also, there were two images of Shah's face on the iPod.

Indictment and Arrest of Brijesh Shah

26. On 10/25/2018, Shah was indicted for 18 U.S.C. § 2251(a)(e) (Production of Child Pornography) and 18 U.S.C. § 2252A(a)(2) and (b)(1) (Receiving Child Pornography), 18 U.S.C. § 2422(b) (Online Enticement), and 18 U.S.C. § 2261A(2) (Cyberstalking). On 11/09/2018, Shah was arrested at his residence in Columbus, Ohio, and detained pending trial in the District of Oregon.

Pretrial Release Violation

27. On 06/22/2021, Shah was placed under pretrial supervision with conditions which include, Shah not possess, obtain or view material which depicts sexually explicit conduct as defined by 18 U.S.C. § 2256, and Shah permit Pretrial Services to install monitoring software on

any computer within the defendant's possession or control that allows random or regular monitoring of the defendant's computer use, and allow Pretrial Services periodic inspection of any such computer including retrieval, copying and review of its electronic contents.

28. On 07/29/2021, Pretrial Services reviewed monitoring software for the Device. The monitoring software had flagged concerning images. Pretrial Services reviewed several screenshots the monitoring software took of Shah's phone. The screenshots included a screenshot taken on 7/20/2021 of KD in a bathroom wearing a towel taking a "selfie." On 07/30/3031, Shah told Pretrial Services that he received a new Samsung cell phone through a friend who added him to their account. When he received the new phone, he synched the phone with his previously existing Google account. Shah said that the photos and chat conversation were from his Google drive as well as the history of conversations with persons through Facebook Messenger.

29. I know data on smart phones like the Device can sync with internet-based backup storage and retain large volumes of data. I know this internet-based backup data can include photos, contacts, text histories, and past communications and that these systems retain this data to restore a phone as a backup. Since Shah has denied any relationship with the victim, any evidence of their communications, and photos of the victim on defendant's device will help to corroborate KD's account of the online exploitation. Since the U.S. Pretrial Services monitoring software detected Shah accessing and viewing a photo of KD, the data sought under this warrant will be helpful to compare against the images from KD's devices that she disclosed sending to Shah, as well as the images of KD recovered from Shah's devices that have already been analyzed. From my review of the images from KD's devices, including a blue iPhone, I believe

that the photo the monitoring software captured is of KD and likely to be one of the photos KD identified that she had sent to Shah.

30. The Device is currently in the lawful possession of United States Pretrial Services. It came into the United States Pretrial Services' possession pursuant to the conditions of Shah's release.

31. The Device is currently in the custody of United States Pretrial Services at 85 Marconi Blvd, Room 512, Columbus, Ohio 43215.

32. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone*. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. *Digital camera.* A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. *Portable media player*. A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. *GPS.* A GPS navigation device uses the Global Positioning System to display its current location. It often contains historical records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated as "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time,

combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

h. *Storage medium.* A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

i. *IP address.* An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

j. *Internet.* The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

33. Based on my training, experience, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the

device.

34. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

35. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because, based on my knowledge, training, and experience, I know:

a. Data on the Device can provide evidence of a file that was once on the Device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the device at a relevant time. Further, forensic evidence on a device can show how and when the device was accessed or used. Such "timeline" information allows the forensic

analyst and investigators to understand the chronological context of access, use, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the device user. Last, forensic evidence on a device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information on a device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a computer (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not

present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

37. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

38. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the

warrant, through the conclusion of the case.

39. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

40. If the Device contains evidence, fruits, or contraband, or is an instrumentality of a crime, the government may retain the Device as evidence, fruits, or contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

41. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

42. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

43. Based on the foregoing, I have probable cause to believe, and I do believe, that the Device described in Attachment A contains evidence of violations of 18 U.S.C. § 2251(a)(e)

(Production of Child Pornography) and 18 U.S.C. § 2252A(a)(2) and (b)(1) (Receiving Child Pornography), 18 U.S.C. § 2422(b) (Online Enticement), and 18 U.S.C. § 2261A(2) (Cyberstalking)., as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Device described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

44. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Paul Maloney (District of Oregon) and AUSA Brian Martinez (Southern District of Ohio). I was informed that AUSA Maloney and AUSA Martinez both hold the opinion that the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

Filter Team

45. In an abundance of caution, a Filter Team will be used to review the data returned from this warrant in the event the data contains any privileged attorney-client communications. The Filter Team will consist of an AUSA and an investigator who are separated from the prosecution team in order to protect a subject's Constitutional and statutory rights by ensuring the prosecution team is not exposed to privileged information. The Filter Team will review the data for privileged material before any member of the prosecution team, identify and remove any privileged material from the data, and only pass non-privileged data to the prosecution team for their investigative purposes. A filter memorandum will identify the members of the respective teams and the potential privileged material, and describe the protocols to be used to prevent disclosure of privileged material to the prosecution team.

Request for Sealing

46. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may cause flight from prosecution, cause destruction of or tampering with evidence, or otherwise seriously jeopardize an investigation. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

Chad Lapp
Special Agent, FBI

Subscribed and sworn to by telephone or other reliable means at 3:24 a.m./p.m. in accordance with Fed. R. Crim. P. 4.1 this 6th day of August, 2021.

HON. ELIZABETH PRESTON DEAVERS
United States Magistrate Judge